

---

---

# **DMSO Security Task -- Security Engineering Update**

**Jan Filsinger  
H.O. Lubbes**

**25 January 1996**

---

# AGENDA

---

- **Security Engineering Task Review**
- **Security Engineering Process**
- **Security Architecture Assumptions**
- **Security Architectures**
- **Next Steps**

---

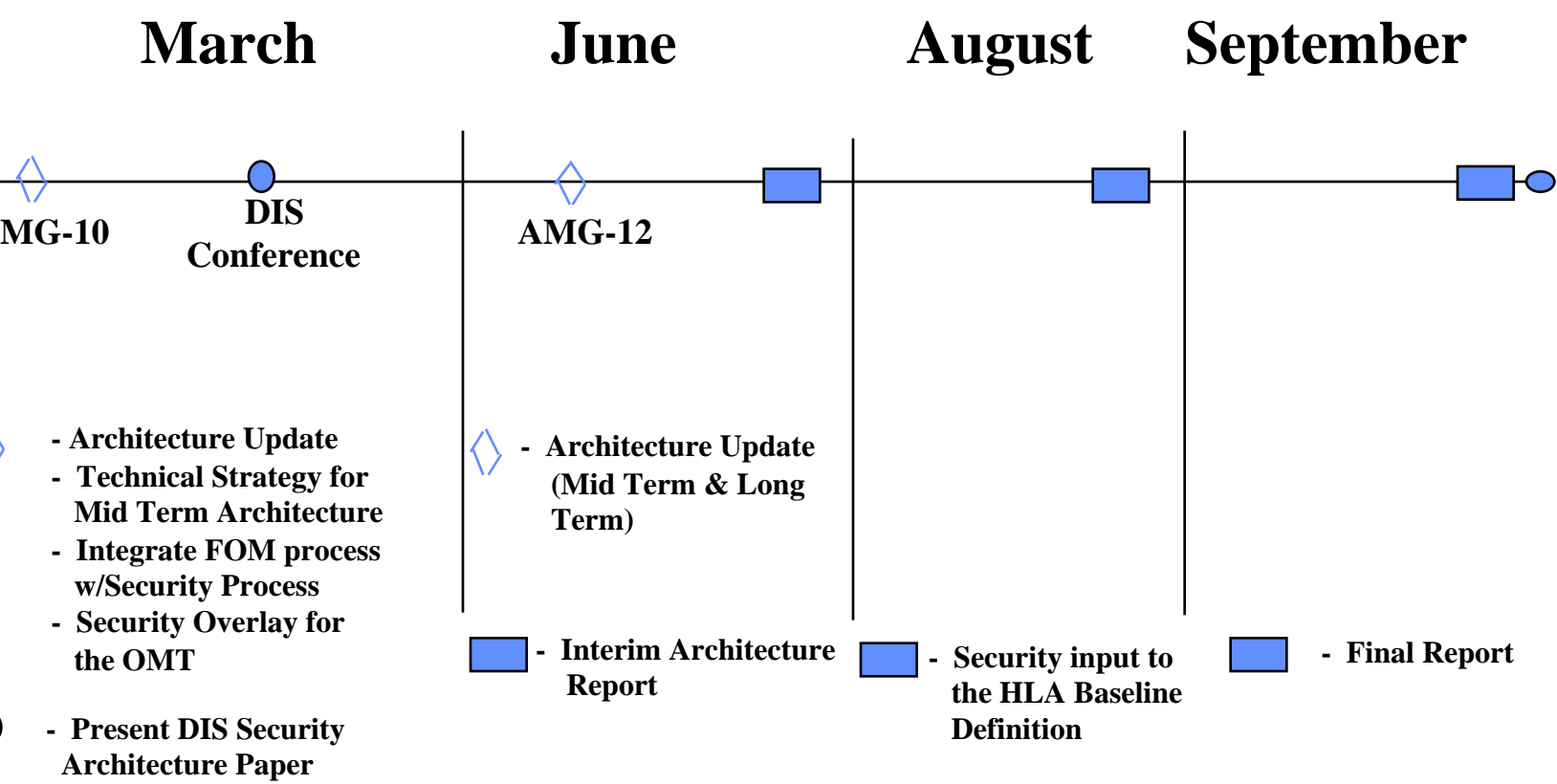
## **Security Engineering Task Review**

---

- **Integrate Security Engineering Activities into the Federation Execution Development Process**
- **Provide Security Overlays to the OMT**
- **Develop Security Architecture for the HLA**
  - **Highlight technical “show stoppers” based on technology assessment**
  - **Results will be incorporated into HLA Baseline**

# Security Engineering Task Review

## Schedule & Milestones



# Security Engineering Process

System Security Engineering Activities	
Engineering Activities	<ul style="list-style-type: none"><li>• Security Concept Definition</li><li>• Security Requirements</li><li>• Security Design</li><li>• Security Implementation</li><li>• Security Verification &amp; Validation</li></ul>
Assurance Activities	<ul style="list-style-type: none"><li>• Evidence Management</li></ul>
Operational Security Risk Activities	<ul style="list-style-type: none"><li>• Risk Management</li><li>• Secure System Operation</li><li>• Configuration Management</li></ul>
Management/Org. Activities	<ul style="list-style-type: none"><li>• Security Coordination</li></ul>

---

## **Security Architecture Assumptions**

---

- **The HLA will provide security mechanisms to protect data and resources. Security within a federate and its private data sources must still be addressed by the individual federate.**
- **The RTI handles all data exchanged among and used by more than one federate.**
- **Sanitization rules are documented.**

---

## **Security Architecture Evolution**

---

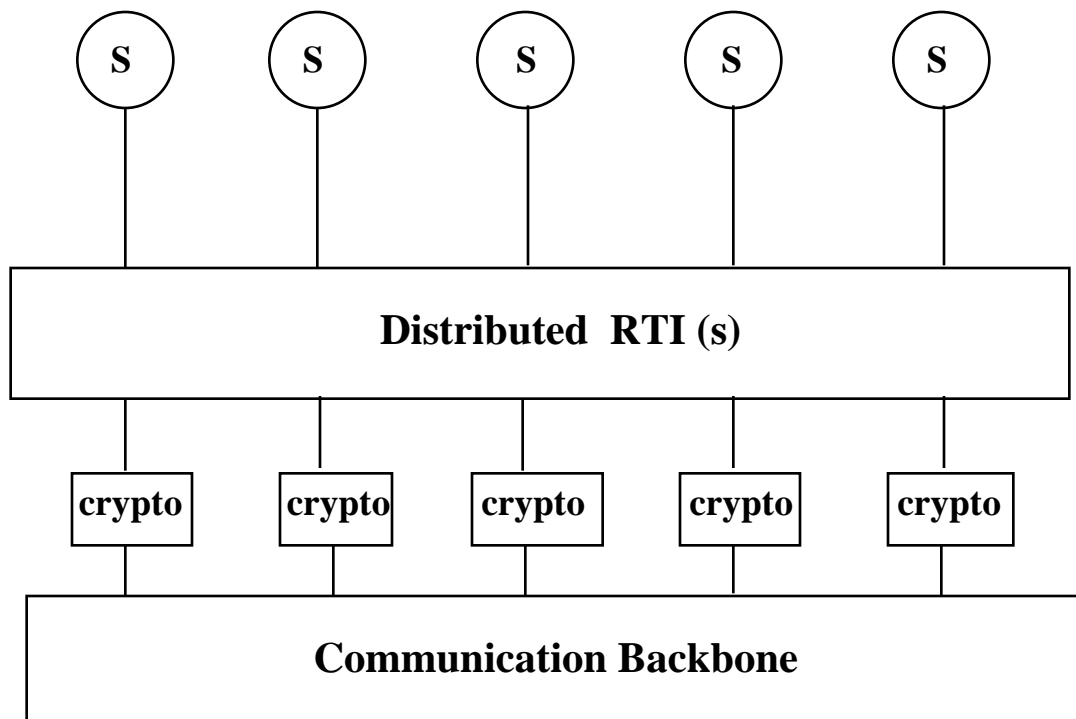
- **Near Term -- Single security level**
- **Long Term -- Multi level secure (MLS)**
- **Mid Term -- Multiple security domains**

# Security Architecture

## Near Term

---

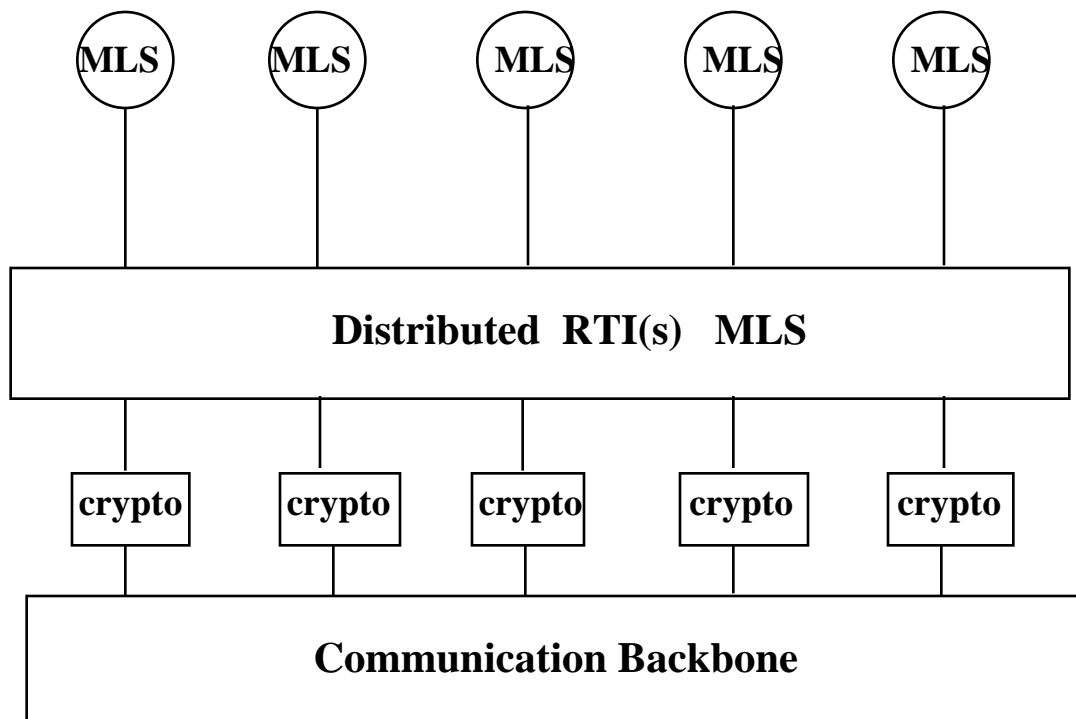
### One Security Level Distributed RTI





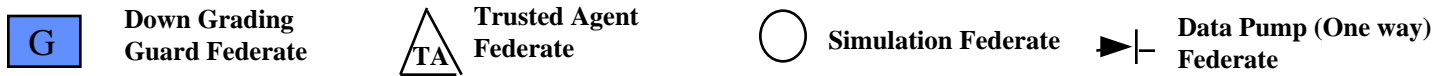
# Security Architecture Long Term

## MLS Simulations and MLS Distributed RTI



---

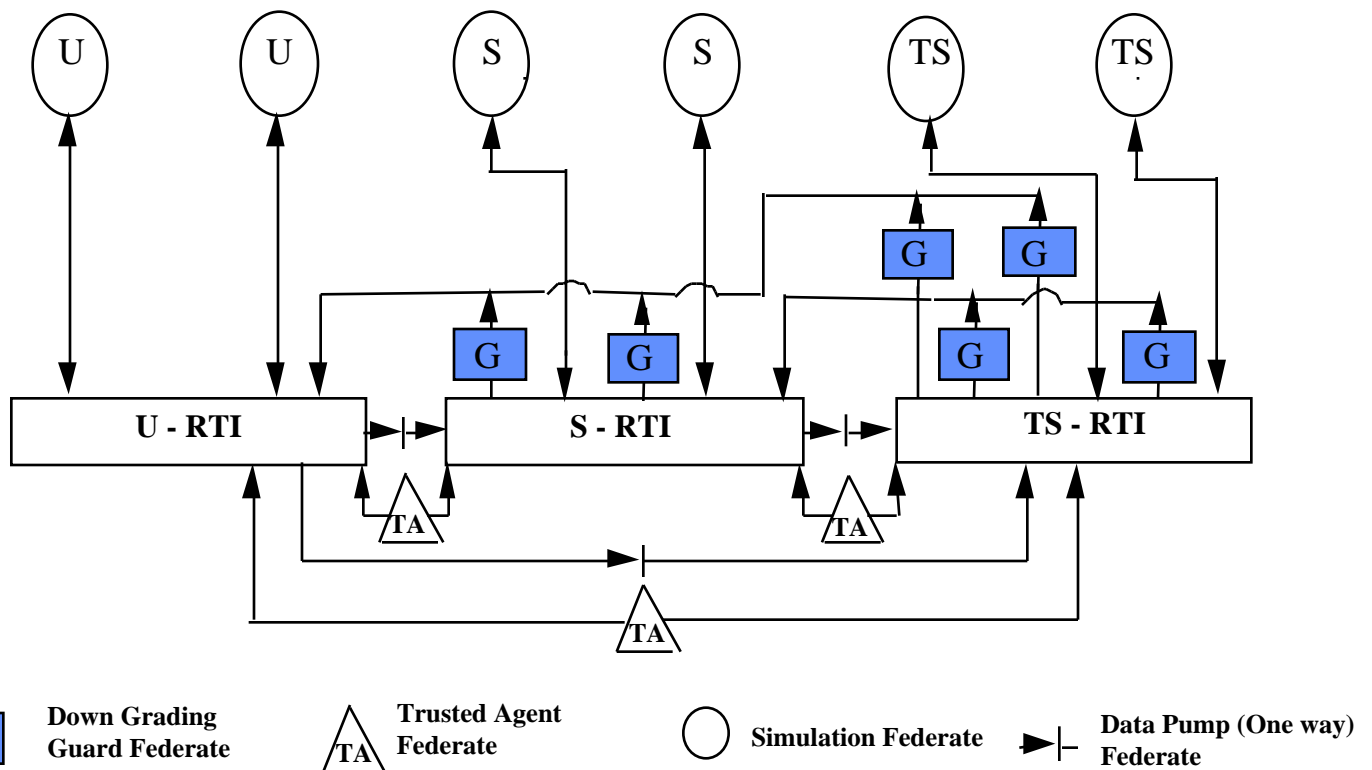
**Federates determine what data is sanitized and to which level based on input from the RTI.**



# Security Architectures

## Mid Term - Option 2

Guards perform sanitization functions.  
The RTI determines what is sanitized and to which level.



# Trade Offs

---

- **Mid term -- option 1 (Federates sanitize data)**
  - **Simplifies security**
    - » **Guards perform check to ensure that sanitization rules were applied correctly**
  - **Federates determine what data is sanitized and to which level based on input from the RTI**
  - **Performance**
    - » **Guards do not become a bottleneck**
  - **Federates can be engineered to sanitize data with little impact to the simulation**
  - **All federates must have a sanitization mechanism built-in to be reusable at different security levels**

## Trade Offs

---

- **Mid term -- option 2 (Guards sanitize data)**
  - The RTI determines what is sanitized and to which level.
  - Complex guard process is a high accreditation risk
    - » May be beyond what is technically feasible
  - Federates are isolated from security functions

---

## Next Steps

---

- **Work to extend the next version of the OMT to include security-relevant information**
- **Study next version of the FOM process and make recommendations for security process integration**
- **Focus on the Mid Term security architecture options**